WEST Search History

| Hide Items | Restore | Clear | Cancel |

DATE: Wednesday, April 11, 2007

Hide?	Set Name	Query	Hit Count
		DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR	
☐	L29	L6 and (polynomial near6 padd$6)	3
☐	L28	L6 and (ntru and OAEP)	2
☐	L27	L25 and (ntru and oaep)	0
☐	L26	L25 and (ntru same oaep)	0
☐	L25	380/30.ccls.	1248
☐	L24	380/30.ccls. and (convert$7 near7 ((injective or (one-to-one))))	1
☐	L22	(convert$7 near7 ((injective or (one-to-one)) same padd$7))	0
☐	L21	ntru and (injective)	2
☐	L20	ntru and OAEP and (injective)	1
☐	L19	ntru and (padd$7 near6 polynomial)	6
☐	L18	(Crypto$7 or encrypt$7) and (padd$6 near7 polynomial)	8
☐	L17	(Crypto$7 or encrypt$7) same (padd$6 near7 polynomial)	1
☐	L16	((oaep and map$8 and polynomial and convert$7 and encrypt$8 and random).clm.)	0
☐	L15	((injective and map$8 and polynomial and convert$7 and encrypt$8 and random).clm.)	1
☐	L14	l6 and (padd$6 near5 polynomial and encrypt$7)	1
☐	L13	padd$6 near5 polynomial and encrypt$7	6
☐	L12	L11 and (l2 or l3 or l4)	0
☐	L11	padd$6 near5 polynomial	31
☐	L10	((oaep and polynomial and convert$7 and random).clm.)	0
☐	L9	((oaep and map$8 and polynomial and convert$7 and encrypt$8 and random).clm.)	0
☐	L8	((injective and map$8 and polynomial and convert$7 and encrypt$8 and random).clm.)	1
☐	L7	((oaep and polynomial).clm.)	1
☐	L6	(380/28,44.ccls.)	2093
☐	L5	(726/$.ccls. and (padding))	191
☐	L4	(726/$.ccls. and OAEP)	7
☐	L3	(380/$.ccls. and OAEP)	16
☐	L2	(713/$.ccls. and OAEP)	26
☐	L1	(((380/28,44.ccls.) or (713/150.ccls.)) and (OAEP and padd$6))	1

END OF SEARCH HISTORY

P⊘RTAL
USPTO

Search: ⦿ The ACM Digital Library ○ The Guide

ntru +"public key"+ OAEP+ polynomial +padding+ injective   **SEARCH**

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Terms used **ntru public key OAEP polynomial padding injective**

Found **135** of **199,915**

| Sort results by | relevance ▽ |
| Display results | expanded form ▽ |

❧ Save results to a Binder
🗎 Search Tips
☐ Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 135   Result page: **1** 2 3 4 5 6 7   next

Relevance scale ☐ ▱ ▬ ▰ ■

1 ## Cryptography and data security
Dorothy Elizabeth Robling Denning
January 1982 Book
Publisher: Addison-Wesley Longman Publishing Co., Inc.

Full text available: 🗎 pdf(19.47 MB)   Additional Information: full citation, abstract, references, citings, index terms

From the Preface (See Front Matter for full Preface)

Electronic computers have evolved from exiguous experimental enterprises in the 1940s to prolific practical data processing systems in the 1980s. As we have come to rely on these systems to process and store data, we have also come to wonder about their ability to protect valuable data.

Data security is the science and study of methods of protecting data in computer and communication systems from unauthorized disclosure ...

2 ## Some facets of complexity theory and cryptography: A five-lecture tutorial
Jörg Rothe
December 2002 **ACM Computing Surveys (CSUR)**, Volume 34 Issue 4
Publisher: ACM Press

Full text available: 🗎 pdf(2.78 MB)   Additional Information: full citation, abstract, references, citings, index terms, review

In this tutorial, selected topics of cryptology and of computational complexity theory are presented. We give a brief overview of the history and the foundations of classical cryptography, and then move on to modern public-key cryptography. Particular attention is paid to cryptographic protocols and the problem of constructing key components of protocols such as one-way functions. A function is one-way if it is easy to compute, but hard to invert. We discuss the notion of one-way functions both ...

Keywords: Complexity theory, interactive proof systems, one-way functions, public-key cryptography, zero-knowledge protocols

3 ## Secure Data Publishing and Certificate Management: Tangler: a censorship-resistant publishing system based on document entanglements

Marc Waldman, David Mazières
November 2001 **Proceedings of the 8th ACM conference on Computer and Communications Security CCS '01**
Publisher: ACM Press

Full text available: 📄 pdf(149.02 KB)   Additional Information: full citation, abstract, references, citings, index terms

We describe the design of a censorship-resistant system that employs a unique document storage mechanism. Newly published documents are dependent on the blocks of previously published documents. We call this dependency an *entanglement*. Entanglement makes replication of previously published content an intrinsic part of the publication process. Groups of files, called collections, can be published together and named in a host-independent manner. Individual documents within a collection can ...

4   Efficient revocation and threshold pairing based cryptosystems
Benoît Libert, Jean-Jacques Quisquater
July 2003   **Proceedings of the twenty-second annual symposium on Principles of distributed computing PODC '03**
Publisher: ACM Press

Full text available: 📄 pdf(1.02 MB)   Additional Information: full citation, abstract, references, citings, index terms

Boneh, Ding, Tsudik and Wong recently proposed a way for obtaining fast revocation of RSA keys. Their method consists in using security mediators that keep a piece of each user's private key in such a way that every decrytion or signature operation requires the help of the mediator for the user. Revocation is achieved by instructing the mediator to stop helping the user to sign or decrypt messages. This security architecture, called SEM, gave rise to an identity based mediated RSA scheme (IB-mRS ...

Keywords: Public key cryptosystems, bilinear maps, revocation

5   Privacy and anonymity: Applications of secure electronic voting to automated privacy-preserving troubleshooting
Qiang Huang, David Jao, Helen J. Wang
November 2005 **Proceedings of the 12th ACM conference on Computer and communications security CCS '05**
Publisher: ACM Press
Full text available: 📄 pdf(237.64 KB)   Additional Information: full citation, abstract, references, index terms

Recent work [27, 15] introduced a novel peer-to-peer application that leverages content sharing and aggregation among the peers to diagnose misconfigurations on a desktop PC. This application poses interesting challenges in preserving privacy of user configuration data and in maintaining integrity of troubleshooting results. In this paper, we provide a much more rigorous cryptographic and yet practical solution for preserving privacy, and we investigate and analyze solutions for ensuring integri ...

Keywords: automatic troubleshooting, homomorphic encryption, integrity, privacy, zero knowledge proof

6   Routing: ANODR: anonymous on demand routing with untraceable routes for mobile ad-hoc networks
Jiejun Kong, Xiaoyan Hong
June 2003 **Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing MobiHoc '03**
Publisher: ACM Press

Full text available: pdf(236.79 KB)   Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>, <u>citings</u>, <u>index terms</u>

In hostile environments, the enemy can launch traffic analysis against interceptable routing information embedded in routing messages and data packets. Allowing adversaries to trace network routes and infer the motion pattern of nodes at the end of those routes may pose a serious threat to covert operations. We propose ANODR, an anonymous on-demand routing protocol for mobile ad hoc networks deployed in hostile environments. We address two closely related problems: For *route anonymity*, AN ...

Keywords: anonymity, broadcast, mobile ad-hoc network, on-demand routing, pseudonymity, trapdoor, untraceability

7   OCB: A block-cipher mode of operation for efficient authenticated encryption

Phillip Rogaway, Mihir Bellare, John Black

August 2003 **ACM Transactions on Information and System Security (TISSEC),** Volume 6 Issue 3

Publisher: ACM Press

Full text available: pdf(568.74 KB)   Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>, <u>index terms</u>

We describe a parallelizable block-cipher mode of operation that simultaneously provides privacy and authenticity. OCB encrypts-and-authenticates a nonempty string $M \in$ {0, 1}* using $\Box \vert M \vert / n \Box$ + 2 block-cipher invocations, where n is the block length of the underlying block cipher. Additional overhead is small. OCB refines a scheme, IAPM, suggested by Charanjit Jutla. Desirable properties of OCB include the ability to encrypt a bi ...

Keywords: AES, authenticity, block-cipher usage, cryptography, encryption, integrity, modes of operation, provable security, standards

8   NP might not be as easy as detecting unique solutions

Richard Beigel, Harry Buhrman, Lance Fortnow

May 1998 **Proceedings of the thirtieth annual ACM symposium on Theory of computing STOC '98**

Publisher: ACM Press

Full text available: pdf(802.68 KB)   Additional Information: <u>full citation</u>, <u>references</u>, <u>citings</u>, <u>index terms</u>

9   Authentication and signature schemes: Efficiency improvements for signature schemes with tight security reductions

Jonathan Katz, Nan Wang

October 2003 **Proceedings of the 10th ACM conference on Computer and communications security CCS '03**

Publisher: ACM Press

Full text available: pdf(306.91 KB)   Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>, <u>index terms</u>

Much recent work has focused on constructing *efficient* digital signature schemes whose security is *tightly* related to the hardness of some underlying cryptographic assumption. With this motivation in mind, we show here two approaches which improve both the computational efficiency and signature length of some recently-proposed schemes:**Diffie-Hellman signatures.** Goh and Jarecki [18] recently analyzed a signature scheme which has a tight security reduction to the computational ...

Keywords: digital signatures

10 Secure routing and firewall: Identity-based registry for secure interdomain routing

E-yong Kim, Klara Nahrstedt, Li Xiao, Kunsoo Park

March 2006 **Proceedings of the 2006 ACM Symposium on Information, computer and communications security ASIACCS '06**

Publisher: ACM Press

Full text available: pdf(320.80 KB)   Additional Information: full citation, abstract, references, index terms

The current Internet has no secure way to validate the correctness of the routing information. We suggest a mechanism that supports secure validation of routing information in the interdomain routing protocol of the Internet. Our mechanism focuses on alleviating obstacles which previously prevent the complete and correct construction of the Internet routing information. In particular, we propose an *identity-based Registry with Authorized and Verifiable Search* (RAVS) so that routing inform ...

Keywords: authorized search, identity-based registry, verifiable search

11 Computer security (SEC): Efficient Diffie-Hellmann two-party key agreement protocols based on elliptic curves

Maurizio Adriano Strangio

March 2005 **Proceedings of the 2005 ACM symposium on Applied computing SAC '05**

Publisher: ACM Press

Full text available: pdf(234.27 KB)   Additional Information: full citation, abstract, references, index terms

Key agreement protocols are of fundamental importance for ensuring the confidentiality of communications between two (or more) parties over an insecure network. In this paper we review existing two-party protocols whose security rests upon the intractability of Diffie-Hellmann and Discrete Logarithm problems over elliptic curve groups. In addition, we propose a new two-party mutual authenticated key agreement protocol and collectively evaluate the security and performance of all the schemes cons ...

Keywords: cryptography, elliptic curves, key agreement, protocols

12 Privacy issues in practice: Coercion-resistant electronic elections

Ari Juels, Dario Catalano, Markus Jakobsson

November 2005 **Proceedings of the 2005 ACM workshop on Privacy in the electronic society WPES '05**

Publisher: ACM Press

Full text available: pdf(165.24 KB)   Additional Information: full citation, abstract, references, index terms

We introduce a model for electronic election schemes that involves a more powerful adversary than previous work. In particular, we allow the adversary to demand of coerced voters that they vote in a particular manner, abstain from voting, or even disclose their secret keys. We define a scheme to be *coercion-resistant* if it is infeasible for the adversary to determine if a coerced voter complies with the demands. A first contribution of this paper is to describe and characterize a new and s ...

Keywords: coercion-resistance, electronic voting, mix networks, receipt-freeness

13 Group Key Management and Signatures: Provably authenticated group Diffie-Hellman key exchange

Emmanuel Bresson, Olivier Chevassut, David Pointcheval, Jean-Jacques Quisquater

November 2001 **Proceedings of the 8th ACM conference on Computer and**

Communications Security CCS '01
Publisher: ACM Press

Full text available: 📄 pdf(578.14 KB)　　Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>, <u>citings</u>, <u>index terms</u>

Group Diffie-Hellman protocols for Authenticated Key Exchange (AKE) are designed to provide a pool of players with a shared secret key which may later be used, for example, to achieve multicast message integrity. Over the years, several schemes have been offered. However, no formal treatment for this cryptographic problem has ever been suggested. In this paper, we present a security model for this problem and use it to precisely define AKE (with "implicit" authentication) as the fundamental goal ...

14 <u>Flash mixing</u>

Markus Jakobsson
May 1999 **Proceedings of the eighteenth annual ACM symposium on Principles of distributed computing PODC '99**
Publisher: ACM Press

Full text available: 📄 pdf(962.64 KB)　　Additional Information: <u>full citation</u>, <u>references</u>, <u>citings</u>, <u>index terms</u>

15 <u>Cryptographic tools: Versatile padding schemes for joint signature and encryption</u>

Yevgeniy Dodis, Michael J. Freedman, Stanislaw Jarecki, Shabsi Walfish
October 2004 **Proceedings of the 11th ACM conference on Computer and communications security CCS '04**
Publisher: ACM Press

Full text available: 📄 pdf(203.91 KB)　　Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>, <u>index terms</u>

We propose several highly-practical and optimized constructions for joint signature and encryption primitives often referred to as <i>signcryption</i>. All our signcryption schemes, built directly from trapdoor permutations such as RSA, share features such as simplicity, efficiency, generality, near-optimal exact security, flexible and ad-hoc key management, key reuse for sending/receiving data, optimally-low message expansion, "backward" use for plain signature/encryption, long messa ...

Keywords: extractable commitments, feistel transform, joint signature and encryption, signcryption, universal padding schemes

16 <u>The isomorphism conjecture fails relative to a random oracle</u>

Stuart A. Kurtz, Stephen R. Mahaney, James S. Royer
March 1995 **Journal of the ACM (JACM)**, Volume 42 Issue 2
Publisher: ACM Press

Full text available: 📄 pdf(1.38 MB)　　Additional Information: <u>full citation</u>, <u>references</u>, <u>citings</u>, <u>index terms</u>, <u>review</u>

Keywords: conjecture, isomorphism, randomness

17 <u>A digital multisignature scheme using bijective public-key cryptosystems</u>

Tatsuaki Okamoto
November 1988 **ACM Transactions on Computer Systems (TOCS)**, Volume 6 Issue 4
Publisher: ACM Press

Full text available: 📄 pdf(640.51 KB)　　Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>, <u>citings</u>, <u>index terms</u>, <u>review</u>

A new digital multisignature scheme using bijective public-key cryptosystems that overcomes the problems of previous signature schemes used for multisignatures is proposed. The principal features of this scheme are (1) the length of a multisignature message is nearly equivalent to that for a singlesignature message; (2) by using a one-way hash function, multisignature generation and verification are processed in an efficient manner; (3) the order of signing is not restricted; and (4) this s ...

18 **Magic Functions: In Memoriam: Bernard M. Dwork 1923--1998**
Cynthia Dwork, Moni Naor, Omer Reingold, Larry Stockmeyer
November 2003 **Journal of the ACM (JACM)**, Volume 50 Issue 6
Publisher: ACM Press

Full text available: pdf(708.05 KB)   Additional Information: full citation, abstract, references, citings, index terms

We prove that three apparently unrelated fundamental problems in distributed computing, cryptography, and complexity theory, are essentially the same problem. These three problems and brief descriptions of them follow. (1) *The selective decommitment problem.* An adversary is given commitments to a collection of messages, and the adversary can ask for some subset of the commitments to be opened. The question is whether seeing the decommitments to these open plaintexts allows the adversary t ...

Keywords: Digital signature, Fiat-Shamir methodology, interactive argument, interactive proof system, magic function, selective decommitment, zero knowledge

19 **The ismorphism conjecture fails relative to a random oracle**
S. A. Kurtz, S. R. Mahaney, J. S. Royer
February 1989 **Proceedings of the twenty-first annual ACM symposium on Theory of computing STOC '89**
Publisher: ACM Press

Full text available: pdf(1.09 MB)   Additional Information: full citation, abstract, references, citings, index terms

Berman and Hartmanis [BH77] conjectured that there is a polynomial-time computable isomorphism between any two languages m-complete ("Karp" complete) for NP. Joseph and Young [JY85] discovered a structurally defined class of NP-complete sets and conjectured that certain of these sets (the Kk_f's) are not isomorphic to the standard NP-complete sets for some one-way functions f. These two conjectures cannot both b ...

20 **How to sign given any trapdoor permutation**
Mihir Bellare, Silvio Micali
January 1992 **Journal of the ACM (JACM)**, Volume 39 Issue 1
Publisher: ACM Press

Full text available: pdf(1.39 MB)   Additional Information: full citation, abstract, references, citings, index terms, review

A digital signature scheme is presented, which is based on the existence of any trapdoor permutation. The scheme is secure in the strongest possible natural sense: namely, it is secure against existential forgery under adaptive chosen message attack.

Keywords: cryptography, digital signatures, randomness, trapdoor functions

Results 1 - 20 of 135   Result page: **1** 2 3 4 5 6 7 next

Useful downloads: Adobe Acrobat   QuickTime   Windows Media Player   Real Player